Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services

Title	Ghost Riders: Sybil Attacks on Crowdsourced Mobile Mapping Services
Publication Type	Journal Article
Year of Publication	2018
Authors	Wang, G., Wang, B., Wang, T., Nika, A., Zheng, H., Zhao, B. Y.
Journal	IEEE/ACM Transactions on Networking
Volume	26
Pagination	1123?1136
ISSN	1063-6692
Keywords	Accidents, automatic user traffic rerouting, cartography, co-location edges, composability, crowdsourced mobile mapping services, crowdsourcing, data privacy, false congestion, ghost riders, Global Positioning System, Google, Google team, graph theory, large proximity graphs, large-scale simulations, location privacy, map systems, Metrics, mobile computing, Mobile handsets, one-time physical co-location, online social networks, points-of-interest, privacy , privacy attacks, pubcrawl, real-time crowdsourced maps, Real-time Systems, Roads, security attacks, single Sybil device, software-based Sybil devices, strong location authentication, Sybil attack, sybil attacks, telecommunication security, traffic engineering computing, virtual vehicles, Waze

Abstract

Real-time crowdsourced maps, such as Waze provide timely updates on traffic, congestion, accidents, and points of interest. In this paper, we demonstrate how lack of strong location authentication allows creation of software-based Sybil devices that expose crowdsourced map systems to a variety of security and privacy attacks. Our experiments show that a single Sybil device with limited resources can cause havoc on Waze, reporting false congestion and accidents and automatically rerouting user traffic. More importantly, we describe techniques to generate Sybil devices at scale, creating armies of virtual vehicles capable of remotely tracking precise movements for large user populations while avoiding detection. To defend against Sybil devices, we propose a new approach based on co-location edges, authenticated records that attest to the one-time physical co-location of a pair of devices. Over time, co-location edges combine to form large proximity graphs that attest to physical interactions between devices, allowing scalable detection of virtual vehicles. We demonstrate the efficacy of this approach using large-scale simulations, and how they can be used to dramatically reduce the impact of the attacks. We have informed Waze/Google team of our research findings. Currently, we are in active collaboration with Waze team to improve the security and privacy of their system.

DOI 10.1109/TNET.2018.2818073

Citation Key wang_ghost_2018

traffic engineering computing data privacy telecommunication security mobile computing real-time systems pubcrawl composability Sybil attack Accidents automatic user traffic rerouting cartography co-location edges crowdsourced mobile mapping services crowdsourcing false congestion ghost riders Global Positioning System Google Google team graph theory large proximity graphs large-scale simulations location privacy map systems Mobile handsets one-time physical co-location online social networks points-of-interest privacy privacy attacks real-time crowdsourced maps Roads security attacks single Sybil device software-based Sybil devices strong location authentication sybil attacks virtual vehicles Waze Metrics